Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Avant Browser Avant Browser 10.0 Build 029, 9.0, 8.0.2	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Avant Browser Dialog Box Origin Spoofing	Medium	Security Focus, 14012, June 21, 2005
BlueCollar Productions iGallery 3.3	A vulnerability has been reported in i-Gallery, which could let a remote user to conduct Cross-Site Scripting and directory traversal. No workaround or patch available at time of publishing. A exploit has been published.	BlueCollar Productions i-Gallery Cross-Site Scripting & Directory Traversal CAN-2005-2033 CAN-2005-2034	Low	Security Focus, 14000, June 20, 2005
Coolcafe Cool Cafe Chat 1.2.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'login.asp' script due tp insufficient validation of user-supplied input, which could let a remote malicious user inject SQL commands; and a vulnerability was reported in 'modifyUser.asp,' which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A exploit has been published.	CoolCafe 'login.asp' SQL Injection & Information Disclosure CAN-2005-2035 CAN-2005-2036	Medium	Exploit Labs, EXPL-A-2005-009
Fortibus Fortibus CMS 4.0.0	Several vulnerabilities have been reported: multiple SQL injection vulnerabilities were reported in Fortibus CMS, which could let a remote malicious user to execute SQL commands; and a vulnerability was reported because a remote malicious user can modify information via the 'My info' page. The vendor has released a patch. No exploit is required.	Fortibus CMS SQL Injection & Information Modification CAN-2005-2037 CAN-2005-2038	High	Security Tracker Alert, 1014242, June 20 2005

Microsoft ASP.NET 1.x	A vulnerability exists which can be exploited a malicious user to bypass security restrictions. The vulnerability is caused by a canonicalization error within the .NET authentication schema. Apply ASP.NET ValidatePath module: http://www.microsoft.com/downloads/details.aspx?FamilyId=DA77B852-DFA0-4631-AAF9-8BCC6C743026 Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-004.mspx **Availability of an updated package for .NET Framework 1.0 Service Pack 3 for the following operating system Versions: Windows XP Tablet PC Edition and Windows XP Media Center Edition.** A Proof of Concept exploit has been published.	Microsoft ASP.NET Canonicalization CAN-2004-0847	Medium	Microsoft, October 7, 2004 Microsoft Security Bulletin, MS05-004, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Vulnerability Note VU#283646 **Microsoft Security Bulletin, MS05-004 V2.0, June 14, 2005**
Microsoft Microsoft Internet Explorer 6.0, SP1&SP2	A vulnerability has been reported in Microsoft Internet Explorer, which could let malicious websites to spoof dialog boxes. No workaround or patch available at time of publishing. Currently we are not aware of any exploit for this vulnerability.	Microsoft Internet Explorer Dialog Origin Spoofing	Low	Secunia, Advisory, SA15491, June 21, 2005
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP 1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, Windows 98 SE, and Windows ME	Multiple vulnerabilities have been reported that include IP Validation, ICMP Connection Reset, ICMP Path MTU, TCP Connection Reset, and Spoofed Connection Request. These vulnerabilities could let remote malicious users execute arbitrary code or execute a Denial of Service. Updates available: http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx **A revised version of the security update is available. Microsoft recommends installing this revised security update even if you have installed the previous version. The revised security update will be available through Windows.** Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities CAN-2005-0048 CAN-2004-0790 CAN-2004-1060 CAN-2004-0230 CAN-2005-0688	High	Microsoft Security Bulletin MS05-019, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#233754 **Microsoft Security Bulletin MS05-019 V 2.0, June 14, 2005**
Novell Novell GroupWise 5.5, 6.0, 6.5.2	A vulnerability has been reported in Novell GroupWise, which could let a local user to obtain a target user's email password. No workaround or patch available at time of publishing. No exploit is required.	Novell GroupWise Client Local Password Disclosure	Medium	Security Tracker, Alert, 1014247, June 20 2005
UApplication UBlog Reload 1.0.5	Multiple vulnerabilities were reported in UBlog Reload, which which could let a remote user to execute SQL commands or perform cross site scripting. There is no solution available at the time of publishing. No exploit is required.	Ublog Reload SQL Injection & Cross-SIte Scripting CAN-2005-2009 CAN-2005-2010	Medium	Security Focus, 13994, June 20 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache SpamAssassin 3.0.1, 3.0.2, 3.0.3	A vulnerability has been reported that could let remote malicious users cause a Denial of Service. A remote user can send e-mail containing special message headers to cause the application to take an excessive	Apache SpamAssassin Lets Remote Users Deny Service	Low	Security Tracker Alert ID: 1014219, June 16, 2005

	amount of time to check the message. A fixed version (3.0.4) is available at: http://spamassassin.apache.org/downloads.cgi Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200506-17.xml There is no exploit code required.	CAN-2005-1266		Fedora Update Notifications, FEDORA-2005-427 & 428, June 16 & 17, 2005 Gentoo Linux Security Advisory, GLSA 200506-17, June 21, 2005
Apple Safari 1.x	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Apple Safari Dialog Box Origin Spoofing	Medium	Secunia Advisory, SA15474, June 21, 2005
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when the application processes malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-474.html** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:015, June 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 **RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005**

bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/b/bzip2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-474.html** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Debian Security Advisory, DSA 730-1, May 27, 2005 Turbolinux Security Advisory , TLSA-2005-60, June 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 **RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005**
cPanel Inc. cPanel 9.1, 9.0, 8.0, 7.0, 6.4-6.4.2, 6.2, 6.0, 5.3, 5.0	A Cross-Site Scripting vulnerability has been reported in the 'login' page due to insufficient sanitization of the 'user' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	cPanel 'User' Parameter Cross-Site Scripting CAN-2005-2021	High	Security Focus, 13996, June 20, 2005
Edgewall Software Trac 0.8.3, 0.7.1	A vulnerability has been reported in the 'id' parameter when processing an attachment upload and download request, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://ftp.edgewall.com/pub/trac/trac-0.8.4.tar.gz There is no exploit code required.	Edgewall Software Trac Arbitrary File Upload/Download CAN-2005-2007	Medium	Secunia Advisory, SA15752, June 20, 2005
Gentoo Linux 1.x	A vulnerability was reported in the webapp-config utility because the 'fn_show_postinst()' function creates a temporary file in an unsafe manner, which could let a malicious user obtain root privileges. The vendor has released a fixed version of net-www/webapp-config (1.10-r14). **Gentoo:** **http://security.gentoo.org/glsa/glsa-200506-13.xml** A Proof of Concept exploit has been published.	Gentoo webapp-config Insecure Temporary File CAN-2005-1707	High	Security Tracker Alert, 1014027, May 22, 2005 **Gentoo Linux Security Advisory, GLSA 200506-13, June 17, 2005**

GNOME gEdit 2.0.2, 2.2 .0, 2.10.2	A format string vulnerability has been reported when invoking the program with a filename that includes malicious format specifiers, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/g/gedit/ Gentoo: http://security.gentoo.org/ glsa/glsa-200506-09.xml RedHat: http://rhn.redhat.com/ errata/RHSA-2005-499.html **Mandriva:** **http://www.mandriva.com/ security/advisories** An exploit has been published.	Gedit Filename Format String CAN-2005-1686	High	Securiteam, May 22, 2005 Ubuntu Security Notice, USN-138-1, June 09, 2005 Gentoo Linux Security Advisory, GLSA 200506-09, June 11, 2005 RedHat Security Advisory, RHSA-2005:499-05, June 13, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:102, June 16, 2005**
GNU a2ps 4.13b	Two vulnerabilities exist in GNU a2ps, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerabilities are caused due to the fixps.in and psmandup.in scripts creating temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running a vulnerable script. Debian: http://security.debian.org/ pool/updates/main/a/a2ps/ Gentoo: http://security.gentoo.org/ glsa/glsa-200501-02.xml Mandriva: http://www.mandriva.com/ security/advisories **TurboLlinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for these vulnerabilities.	GNU a2ps Two Scripts Insecure Temporary File Creation CAN-2004-1377	Medium	Secunia SA13641, December 27, 2004 Gentoo Linux Security Advisory, GLSA 200501-02, January 4, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:097, June 7, 2005 **Turbolinux Security Advisory, TLSA-2005-64, June 15, 2005**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200506-16.xml** A Proof of Concept exploit has been published.	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005 **Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005**
GNU sharutils 4.2, 4.2.1; **Avaya S8710 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8500 R2.0.1, S8500 R2.0.0, S8300 R2.0.1, R2.0.0, Modular Messaging (MSS) 2.0, 1.1,** **Avaya MN100, Intuity LX,** **Avaya Converged Communications Server 2.0**	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200410-01.xml FedoraLegacy: http://download.fedoralegacy.	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	High	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004 Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005 Ubuntu Security Notice, USN-102-1 March 29, 2005

	org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-377.html Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-135_RHSA-2005-377.pdf** We are not aware of any exploits for these vulnerabilities.		Fedora Update Notifications, FEDORA-2005-280 & 281, April 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005 Turbolinux Security Advisory, TLSA-2005-54, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Avaya Security Advisory, ASA-2005-135, June 14, 2005**

GNU sharutils 4.2, 4.2.1; **Avaya S8710 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8500 R2.0.1, S8500 R2.0.0, S8300 R2.0.1, R2.0.0, Modular Messaging (MSS) 2.0, 1.1,** **Avaya MN100, Intuity LX,** **Avaya Converged Communications Server 2.0**	A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-377.html Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-135_RHSA-2005-377.pdf** There is no exploit code required.	GNU Sharutils 'Unshar' Insecure Temporary File Creation CAN-2005-0990	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005 Gentoo Linux Security Advisory, GLSA 200504-06, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 Fedora Update Notification, FEDORA-2005-319, April 14, 2005 RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005 Turbolinux Security Advisory, TLSA-2005-54, April 28, 200 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Avaya Security Advisory, ASA-2005-135, June 14, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit script has been published.	GNU wget File Creation & Overwrite CAN-2004-1487 CAN-2004-1488	Medium	Security Tracker Alert ID: 1012472, December 10, 2004 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:098, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 **Turbolinux Security Advisory, TLSA-2005-66, June 15, 2005**

GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-474.html** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 **RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005**
iCab iCab 2.9.8	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	iCab Web Browser Dialog Box Origin Spoofing	Medium	Secunia Advisory, SA15477, June 21, 2005
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3; IPCop 1.4.1, 1.4.2, 1.4.4, 1.4.5	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-06.xml Mandriva: http://www.mandriva.com/security/advisories IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD FreeBSD:	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 Fedora Update Notification, FEDORA-2005-351, May 3, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Ubuntu Security Notice, USN-119-1 May 06, 2005 Gentoo Linux Security Advisory, GLSA 200505-06, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:087, May 12, 2005 Security Focus, 13392, May 12, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:10, June 9, 2005 **Avaya Security Advisory, ASA-2005-137, June 13, 2005** **Turbolinux Security Advisory,TLSA-2005-63, June 15, 2005**

	ftp://ftp.FreeBSD.org/pub/ FreeBSD/CERT/patches/ SA-05:10/tcpdump.patch **Avaya:** **http://support.avaya.com/ elmodocs2/security/ ASA-2005-137_ RHSA-2005-417_ RHSA-2005-421.pdf** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/** Exploit scripts have been published.			
Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. A fixed version (5.8.4 or later) is available at: http://www.perl.com/CPAN/src/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/ glsa-200501-38.xml Debian: http://security.debian.org/pool /updates/main/p/perl/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php **HP:** **http://software.hp.com/** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005 **HP Security Bulletin, HPSBUX01208, June 16, 2005**
Multiple Vendors RedHat Fedora Core3; LBL tcpdump 3.9.1, 3.9, 3.8.1-3.8.3, 3.7-3.7.2, 3.6.3, 3.6.2, 3.5.2, 3.5, alpha, 3.4, 3.4 a6	A remote Denial of Service vulnerability has been reported in the 'bgp_update_print()' function in 'print-bgp.c' when a malicious user submits specially crafted BGP protocol data. Update available at: http://cvs.tcpdump.org/cgi-bin/ cvsweb/tcpdump/print-bgp.c Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ Trustix: ftp://ftp.trustix.org/pub/trustix/ updates/ **Mandriva:** **http://www.mandriva.com/**	TCPDump BGP Decoding Routines Denial of Service CAN-2005-1267	Low	Security Tracker Alert, 1014133, June 8, 2005 Fedora Update Notification, FEDORA-2005-406, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:101, June 15, 2005** **Fedora Update Notification, FEDORA-2005-407, June 16, 2005** **Ubuntu Security Notice, USN-141-1, June 21, 2005**

	security/advisories **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/4/** **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/t/tcpdump/** A Proof of Concept exploit script has been published.			
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE9, .STABLE8, .STABLE7	A vulnerability exists when using the Netscape Set-Cookie recommendations for handling cookies in caches due to a race condition, which could let a malicious user obtain sensitive information. Patches available at: http://www.squid-cache.org/Versions /v2/2.5/bugs/squid-2.5.STABLE9-setcookie.patch Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/s/squid/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes. conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-415.html** There is no exploit code required.	Squid Proxy Set-Cookie Headers Information Disclosure CAN-2005-0626	Medium	Secunia Advisory, SA14451, March 3, 2005 Ubuntu Security Notice, USN-93-1 March 08, 2005 Fedora Update Notifications, FEDORA-2005- 275 & 276, March 30, 2005 Conectiva Linux Security Announcement, CLA-2005:948, April 27, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:078, April 29, 2005 **RedHat Security Advisory, RHSA-2005:415-16, June 14, 2005**
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1; **Avaya Modular Messaging (MSS) 2.0, 1.1** **Avaya MN100,** **Avaya Intuity LX** **ALT Linux ALT Linux Junior 2.3,** **ALT Linux ALT Linux Compact 2.3**	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200503-05.xml Debian: http://security.debian.org/ pool/updates/main/x/xli/ Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/ RHSA-2005-332.html Mandrake: http://www.mandrakesecure.net/	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 Turbolinux Security Advisory, TLSA-2005-43, April 19, 2005 RedHat Security Advisory, RHSA-2005:332-10, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:076, April 21, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Avaya Security Advisory, ASA-2005-134, June 14, 2005**

	en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-134_RHSA-2005-332.pdf** Currently we are not aware of any exploits for this vulnerability.			
NanoBlogger NanoBlogger 3.2.1, 3.2	A vulnerability has been reported in some plugins because certain input files are invoked insecurely, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://nanoblogger.sourceforge.net/downloads/nanoblogger-3.2.3.tar.gz Currently we are not aware of any exploits for this vulnerability.	NanoBlogger Remote Arbitrary Command Execution CAN-2005-2039	High	Secunia Advisory, SA15754, June 21, 2005
Novell NetMail 3.52 A-C	A vulnerability has been reported in the Owner and Group ID files in the NetMail patches because they are incorrectly set to 500, which could let malicious user user delete/replace NetMail binaries. Patches available at: http://support.novell.com/servlet/filedownload/sec/pub/netmail352c1_li n.tgz There is no exploit code required.	Novell NetMail Insecure Patch File Permissions CAN-2005-1976	Medium	Novell TID, 10098022, June 17, 2005
OpenBSD 3.6, 3.7	A vulnerability has been reported that could let a local user cause a Denial of Service. A local user can invoke getsockopt(2) to get ipsec(4) credentials for a socket to trigger a kernel panic. The flaw resides in 'sys/netinet/ip_output.c' in the ip_ctloutput() function. The vendor has issued the following fixes: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.7/common/002_getsockopt.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/017_getsockopt.patch Currently we are not aware of any exploits for this vulnerability.	OpenBSD IPSec getsockopt() Denial of Service	Low	OpenBSD 3.6 and 3.7 Release Errata, June 15, 2005
php Arena paFileDB 3.1 and prior	Several input validation vulnerabilities were reported in paFileDB that could let a remote malicious user inject SQL commands, conduct Cross-Site Scripting attacks, and view or execute files on the target system. The vendor has issued a fixed version which has the same version number as the vulnerable version. Proofs of Concept exploits have been published.	paFileDB SQL Injection, Cross-Site Scripting & File Disclosure CAN-2005-1999 CAN-2005-2000 CAN-2005-2001	High	Security Tracker Alert, 1014209, June 15, 2005 US-CERT VU#459565

PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A remote Denial of Service vulnerability has been reported when processing deeply nested EXIF IFD (Image File Directory) data. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955 Apple: http://www.apple.com/support/downloads/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-136_RHSA-2005-405_RHSA-2005-406.pdf** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Nesting Remote Denial of Service CAN-2005-1043	Low	Security Focus, 13164, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Conectiva Security Advisory, CLSA-2005:955, May 31, 2005 Apple Security Update, APPLE-SA-2005-06-08, June 8, 2005 **Avaya Security Advisory, ASA-2005-136, June 14, 2005**

PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955 Apple: http://www.apple.com/support/downloads/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-136_RHSA-2005-405_RHSA-2005-406.pdf** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Conectiva Security Advisory, CLSA-2005:955, May 31, 2005 Apple Security Update, APPLE-SA-2005-06-08, June 8, 2005 **Avaya Security Advisory, ASA-2005-136, June 14, 2005**
Rob Flynn Gaim prior to 1.3.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported when using the Yahoo! protocol to download a file; and a remote Denial of Service vulnerability was reported in the MSN Messenger service when a malicious user submits a specially crafted MSN message. Updates available at:	Gaim Remote Denial of Services CAN-2005-1269 CAN-2005-1934	Low	Secunia Advisory, SA15648, June 10, 2005 Ubuntu Security Notice USN-139-1, June 10, 2005 Gentoo Linux Security Advisory, GLSA

	http://gaim.sourceforge.net /downloads.php Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/ glsa/glsa-200506-11.xml Mandriva: http://www.mandriva.com/ security/advisories **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/** **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-518.html** There is no exploit code required.			200506-11, June 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:099, June 14, 2005 **Fedora Update Notifications, FEDORA-2005-410, & 411, June 17, 2005** **RedHat Security Advisory, RHSA-2005:518-03, June 16, 2005**
Royal Institute of Technology Heimdal 0.6-0.6.4, 0.5.0-0.5.3, 0.4 a-f	Multiple buffer overflow vulnerabilities have been reported in the 'getterminaltype()' function due to a boundary error in telnetd, which could let a remote malicious user execute arbitrary code. Upgrades available at: ftp://ftp.pdc.kth.se/pub/heimdal/ src/heimdal-0.6.5.tar.gz Currently we are not aware of any exploits for this vulnerability.	Heimdal TelnetD Remote Buffer Overflow CAN-2005-2040	High	Secunia Advisory, SA15718, June 20, 2005
Sun Microsystems, Inc. Messaging Server 6.2, iPlanet Messaging Server 5.2	A vulnerability has bee reported in in Sun ONE Messaging Server (iPlanet Messaging Server), which could let a remote malicious user execute arbitrary code. *Note: Only target users running Internet Explorer are affected.* No workaround or patch available at time of publishing. There is no exploit code required.	Sun ONE/iPlanet Messaging Server Arbitrary Code Execution CAN-2005-2022	High	Sun(sm) Alert Notification, 101770. June 17, 2005
SuSE SuSE Linux 9.3, x86_64	An unspecified vulnerability was reported when using gpg2 for S/MIME signing. The impact was not specified. SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	SuSE Linux GPG2 S/MIME Signing CAN-2005-2023	Not Specified	SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005
Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9	A race condition vulnerability has been reported when the sudoers configuration file contains a pseudo-command 'ALL' that directly follows a users sudoers entry, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.sudo.ws/sudo/ dist/sudo-1.6.8p9.tar.gz OpenBSD: http://www.openbsd.org/ errata.html There is no exploit code required.	Todd Miller Sudo Local Race Condition CAN-2005-1993	High	Security Focus, 13993, June 20, 2005

Vipul Razor-agents prior to 2.72	Two vulnerabilities have been reported that could let malicious users cause a Denial of Service. This is due to an unspecified error in the preprocessing of certain HTML and an error in the discovery logic. Updates available at: http://prdownloads.sourceforge.net/razor/razor-agents-2.72.tar.gz?down load Gentoo: http://security.gentoo.org/glsa/glsa-200506-17.xml Currently we are not aware of any exploits for these vulnerabilities.	Vipul Razor-agents Denials of Service CAN-2005-2024	Low	Security Focus, Bugtraq ID 13984, June 17, 2005 Gentoo Linux Security Advisory, GLSA 200506-17, June 21, 2005
ViRobot ViRobot Linux Server 2.0	A buffer overflow vulnerability has been reported in the web based management interface due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	ViRobot Linux Server Remote Buffer Overflow CAN-2005-2041	High	Securiteam, June 15, 2005
winace.com UnAce 1.0, 1.1, 1.2 b	Several vulnerabilities exist: a buffer overflow vulnerability exists in the ACE archive due to an incorrect 'strncpy()' call, which could let a remote malicious user execute arbitrary code; two other buffer overflow vulnerabilities exist when archive name command line arguments are longer than 15,600 characters and when printing strings are processed, which could let a remote malicious user execute code; and a Directory Traversal vulnerability exists due to improper filename character processing, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200502-32.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is not exploit code required; however, Proofs of Concept exploits have been published.	Winace UnAce ACE Archive Remote Directory Traversal & Buffer Overflow CAN-2005-0160 CAN-2005-0161	High	Security Tracker Alert, 1013265, February 23, 2005 **SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005**
Yaws Yaws 1.55 and prior	A vulnerability has been reported that could let remote malicious users gain knowledge of sensitive information. This is due to an input validation error when handling a request containing a NULL byte appended to the filename. Update to version 1.56: http://yaws.hyber.org/yaws-1.55_to_1.56.patch There is no exploit code required; however; a Proof of Concept exploit has been published.	Yaws Source Code Disclosure CAN-2005-2008	Medium	SEC-CONSULT Security Advisory, 20050616-0
Yukihiro Matsumoto Ruby 1.8.2	A vulnerability has been reported in the XMLRPC server due to a failure to set a valid default value that prevents security protection using handlers, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	Yukihiro Matsumoto Ruby XMLRPC Server Unspecified Command Execution CAN-2005-1992	High	Fedora Update Notifications, FEDORA-2005-474 & 475, June 21, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Acrobat and Reader 7.0 and 7.0.1 for Mac OS and Windows.	A vulnerability has been reported that could let remote malicious users access system information. This is because there is an error in the Adobe Reader control that makes it possible to determine whether or not a particular file exists on a user's system via XML scripts embedded in JavaScript. Update to version 7.0.2 for Windows: http://www.adobe.com/support/downloads/ Update for Mac OS currently not available. Currently we are not aware of any exploits for this vulnerability.	Adobe Reader / Adobe Acrobat Local File Detection CAN-2005-1306	Medium	Adobe Advisory Document 331710, June 15, 2005
ajax-spell ajax-spell 1.1-1.7	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks. Input passed in HTML tag entities is not properly verified before being returned to users. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=141511&package_i d=155305 There is no exploit code required.	ajax-spell Cross-Site Scripting CAN-2005-2042	High	Secunia SA15737, June 17, 2005
Apache Friends XAMPP 1.4.13	A vulnerability has been reported that could let remote malicious users view potentially sensitive information and conduct script insertion attacks. Input passed to the query string in 'lang.php' isn't properly verified. Update to version 1.4.14: http://sourceforge.net/project/showfiles.php?group_id=61776 There is no exploit code required.	Apache Friends XAMPP 'lang.php' Script Insertion & Information Disclosure CAN-2005-2043	High	Secunia SA15735, June 17, 2005
ATRC ATutor 1.4.3, 1.5 RC 1	A vulnerability has been reported that could let a remote user conduct Cross-Site Scripting attacks. Several scripts do not properly validate user-supplied input. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ATutor Cross-Site Scripting CAN-2005-2044	High	Security Focus Bugtraq ID 13972, June 16, 2005
Bitrix Bitrix Site Manager 4.0.5	Several vulnerabilities have been reported: a vulnerability was reported in 'admin/index.php' due to insufficient validation of the '_SERVER[DOCUMENT_ROOT]' parameter, which could let a remote malicious user include arbitrary files from external and local resources; and a vulnerability was reported because a remote malicious user can obtain sensitive information by accessing certain scripts directly. The vendor has released Bitrix Site Manager 4.0.9 to address this issue. Please contact the vendor to obtain fixes. Currently we are not aware of any exploits for these vulnerabilities.	Bitrix Site Manager File Inclusion & Information Disclosure CAN-2005-1995 CAN-2005-1996	High	Secunia SA15726, June 16, 2005
C1 Financial Services Contelligent 9.0.15	A vulnerability has been reported because a remote authenticated malicious user can invoke the preview mechanism and set a role for which the user is not authorized, which could lead to elevated privileges. Update available at: http://www.contelligent.com/contell/cms/c1web/contelligent/site/contelligent/downloads/index.html Currently we are not aware of any exploits for this vulnerability.	Contelligent Preview Elevated Privileges	Medium	Security Tracker Alert, 1014240, June 19, 2005

Cisco Systems VPN Concentrator 3000 series products running groupname authentication	A vulnerability has been reported due to a design error when responding to valid and invalid groupnames, which could let a malicious user carry out bruteforce attacks against the password hash. Upgrade information available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/4_7/471con3k.htm#wp560292 There is no exploit code required.	Cisco VPN Concentrator Groupname Enumeration CAN-2005-2025	Medium	Security Focus, 13992, June 20, 2005
Claroline Claroline 1.5.3, 1.6 rc1, 1.6 beta; **Dokeos Open Source Learning & Knowledge Management Tool 1.5.5**	Multiple input validation vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported in the '/exercise_result.php,' 'exercice_submit.php,' 'myagenda.php,' 'agenda.php,' 'user_access_details.php,' 'toolaccess_details.php,' 'learningPathList.php,' 'learningPathAdmin.php,' 'learningPath.php,' and 'userLog.php' pages due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code; SQL injection vulnerabilities were reported in 'learningPath.php (3),' 'exercises_details.php,' 'learningPathAdmin.php,' 'learnPath_details.php,' 'userInfo.php (2),' 'modules_pool.php,' and 'module.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary SQL code; multiple Directory Traversal vulnerabilities were reported in 'claroline/document/document.php' and 'claroline/learnPath/insertMyDoc.php' due to insufficient input validation, which could let remote malicious project administrators (teachers) upload files in arbitrary folders or copy/move/delete (then view) files of arbitrary folders; and remote file inclusion vulnerabilities were reported due to insufficient verification, which could let a remote malicious user include arbitrary files from external and local resources. Upgrades available at: http://www.claroline.net/dlarea/ **Dokeos:** **http://www.dokeos.com/download/dokeos-1.6.rc2.zip** There is no exploit code required; however, Proofs of Concept exploits have been published.	Claroline Multiple Vulnerabilities CAN-2005-1374 CAN-2005-1375 CAN-2005-1376 CAN-2005-1377	High	Zone-H Research Center Security Advisory, 200501, April 27, 2005 **Security Focus, 13407, June 16, 2005**
Dirk Krause fig2vect 1.0.1	A vulnerability has been reported that could let remote malicious users execute arbitrary code. This is due to a boundary error in the 'pdf_encode_str()' function. Update to version 1.0.2: http://sourceforge.net/project/showfiles.php?group_id=112082 Currently we are not aware of any exploits for this vulnerability.	Dirk Krause fig2vect 'pdf_encode_str()' Buffer Overflow	High	Secunia SA13637, June 17, 2005
Dokeos Dokeos 1.5.5	Multiple vulnerabilities have been reported which could let remote malicious users conduct Cross-Site Scripting and SQL injection attacks, manipulate, and disclose sensitive information. The vulnerabilities have been fixed in version 1.6 RC2. Currently we are not aware of any exploits for these vulnerabilities.	Dokeos Multiple Vulnerabilities CAN-2005-1374 CAN-2005-1375 CAN-2005-1376 CAN-2005-1377	High	Secunia, SA15725, June 16, 2005
e107.org e107 website system 0.617, 0.616, 0.6 15a, 0.6 15	Multiple vulnerabilities have been reported: a vulnerability was reported because different error messages are returned regarding valid or invalid usernames, which could let a remote malicious user obtain sensitive information; and several Cross-Site Scripting vulnerabilities have been reported due to insufficient input validation before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	e107 Website System Information Disclosure & Cross-Site Scripting	High	Security Focus, 13974, June 16, 2005
Enterasys Networks Vertical Horizon VH-2402S	Several vulnerabilities have been reported: a vulnerability was reported due to an undocumented default account that contains a default password used for debugging purposes, which could let a remote malicious user obtain administrative access; and a vulnerability was reported because	Enterasys Networks Vertical Horizon Default Backdoor	High	Secunia Advisory, SA15757, June 21, 2005

02.05.09.07, VH-2402S 02.05.00	certain debug commands are available for non-administrative users (e.g. guest users). Patches available at: http://www.enterasys.com/download/download.cgi?lib=vh There is no exploit code required.	Account & Debug Command CAN-2005-2026 CAN-2005-2027		
Ethereal Group Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9 **Avaya Converged Communications Server (CCS) 2.x, Avaya S8XXX Media Servers**	Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509. Upgrades available at: http://www.ethereal.com/distribution/ethereal-0.10.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-03.xml Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-427.html Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000963 SuSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-131_RHSA-2005-306_RHSA-2005-427.pdf** An exploit script has been published.	Ethereal Multiple Remote Protocol Dissector Vulnerabilities CAN-2005-1456 CAN-2005-1457 CAN-2005-1458 CAN-2005-1459 CAN-2005-1460 CAN-2005-1461 CAN-2005-1462 CAN-2005-1463 CAN-2005-1464 CAN-2005-1465 CAN-2005-1466 CAN-2005-1467 CAN-2005-1468 CAN-2005-1469 CAN-2005-1470	High	Ethereal Security Advisory, enpa-sa-00019, May 4, 2005 Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:083, May 11, 2005 RedHat Security Advisory, RHSA-2005:427-05, May 24, 2005 Conectiva Security Advisory, CLSA-2005:963, June 6, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 SGI Security Advisory, 20050503-01-U, June 8, 2005 **Avaya Security Advisory, ASA-2005-131, June 13, 2005**
Ethereal Group Ethereal 0.10-0.10.8	A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/	Ethereal Buffer Overflow CAN-2005-0699	High	Security Focus, 12759, March 8, 2005 Security Focus, 12759, March 14, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005

	Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-131_RHSA-2005-306_RHSA-2005-427.pdf** Exploit scripts have been published.			Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005 RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005 Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 **Avaya Security Advisory, ASA-2005-131, June 13, 2005**
Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/e/ethereal/ **Avaya:**	Ethereal Etheric/ GPRS-LLC/IAPP/ JXTA/s Flow Dissector Vulnerabilities CAN-2005-0704 CAN-2005-0705 CAN-2005-0739 CAN-2005-0765 CAN-2005-0766	HIgh	Ethereal Advisory, enpa-sa-00018, March 12, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005 RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005 Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Debian Security Advisory, DSA 718-1, April 28, 2005 **Avaya Security Advisory, ASA-2005-131, June 13, 2005**

	http://support.avaya.com/elmodocs2/security/ASA-2005-131_RHSA-2005-306_RHSA-2005-427.pdf A Denial of Service Proof of Concept exploit script has been published.			
GNU Midnight Commander Project Midnight Commander 4.x	Multiple vulnerabilities exist due to various design and boundary condition errors, which could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-24.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-217.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-512.html** Currently we are not aware of any exploits for these vulnerabilities.	Midnight Commander Multiple Vulnerabilities CAN-2004-1004 CAN-2004-1005 CAN-2004-1009 CAN-2004-1090 CAN-2004-1091 CAN-2004-1092 CAN-2004-1093 CAN-2004-1174 CAN-2004-1175 CAN-2004-1176	High	Security Tracker Alert, 1012903, January 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Gentoo Linux Security Advisory, GLSA 200502-24, February 17, 2005 RedHat Security Advisory, RHSA-2005:217-10, March 4, 2005 **RedHat Security Advisory, RHSA-2005:512-08, June 16, 2005**
GNU mcGallery 1.1	A vulnerability has been reported that could let remote malicious users access sensitive information. Input passed to the 'lang' parameter in 'admin.php' isn't properly verified. No workaround or patch available at time of publishing. Vulnerability may be exploited via a web browser.	GNU mcGallery 'lang' Local File Inclusion CAN-2005-1997	Medium	Secunia SA15727, June 16, 2005
Horde Project Horde 3.0.4 -RC 2	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of the page title in a parent frame window, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://ftp.horde.org/pub/horde/horde-latest.tar.gz **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Horde Application Page Title Cross-Site Scripting CAN-2005-0961	High	Secunia Advisory: SA14730, March 29, 2005 **SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005**
JBoss Group JBoss 4.0.2, 3.2.7, 3.2.2, 3.2.1, 3.0.8	A vulnerability has been reported in the 'org.jboss.web.WebServer' class due to an error in the request handling for RMI code, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	JBoss Information Disclosure CAN-2005-2006	Medium	Secunia Advisory, SA15746, June 20, 2005
Mamboforge Mambo 4.5.2.2 and prior	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. Input passed to the 'user_rating' parameter when voting isn't properly validated. Update to version 4.5.2.3: http://mamboforge.net/frs/?group_id=5 Currently we are not aware of any exploits for this vulnerability.	Mambo 'user_rating' SQL Injection CAN-2005-2002	High	Secunia SA15710, June 15, 2005

MercuryBoard Message Board 1.1.4	An SQL injection vulnerability has been reported in 'Index.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	MercuryBoard 'Index.PHP' Remote SQL Injection CAN-2005-2028	High	Security Focus, 14015, June 21, 2005
Microsoft Internet Explorer Macintosh Edition 5.2.3, 5.2.2, 5.1.1, 5.1	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer for Mac Dialog Box Origin Spoofing	Medium	Secunia Advisory: SA15491, June 21, 2005
Midnight Commander Midnight Commander 4.5.40-4.5.5.52, 4.5.54, 4.5.55	A buffer overflow vulnerability has been reported in the 'insert_text()' function due to insufficient bounds checking, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-512.html** Currently we are not aware of any exploits for this vulnerability.	Midnight Commander 'Insert_Text' Buffer Overflow CAN-2005-0763	High	Debian Security Advisory, DSA 698-1 , March 29, 2005 Turbolinux Security Advisory, TLSA-2005-46, April 19, 2005 **RedHat Security Advisory, RHSA-2005:512-08, June 16, 2005**
Multiple Vendors Squid Web Proxy Cache2.5.STABLE9 & prior	A vulnerability has been reported in the DNS client when handling DNS responses, which could let a remote malicious user spoof DNS lookups. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-dns_query-4.patch Trustix: http://www.trustix.org/errata/2005/0022/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-415.html** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy DNS Spoofing CAN-2005-1519	Medium	Security Focus, 13592, May 11, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Fedora Update Notification, FEDORA-2005-373, May 17, 2005 Ubuntu Security Notice, USN-129-1 May 18, 2005 **RedHat Security Advisory, RHSA-2005:415-16, June 14, 2005**

Multiple Vendors Windows XP, Server 2003 Windows Services for UNIX 2.2, 3.0, 3.5 when running on Windows 2000 **Kerberos V5 Release 1.3.6** **Avaya Intuity LX, Converged Communications Server (CCS) 2.x, MN100, Modular Messaging 2.x, S8XXX Media Servers**	An information disclosure vulnerability has been reported that could let a remote malicious user read the session variables for users who have open connections to a malicious telnet server. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-033.mspx **RedHat:** **ftp://updates.redhat.com/enterprise** **Microsoft:** **http://www.microsoft.com/technet/security/Bulletin/MS05-033.mspx** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-145_RHSA-2005-504.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Telnet Client Information Disclosure CAN-2005-1205 CAN-2005-0488	Medium	Microsoft, MS05-033, June 14, 2004 US-CERT VU#800829 **iDEFENSE Security Advisory, June 14, 2005** **Red Hat Security Advisory, RHSA-2005:504-00, June 14, 2005** **Microsoft Security Bulletin, MS05-033 & V1.1, June 14 & 15, 2005** **SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005** **Avaya Security Advisory, ASA-2005-145, June 17, 2005**

Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386 SGI IRIX 6.5.24-6.5.27	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005 SGI Security Advisory, 20050405-01-P, May 26, 2005 Debian Security Advisory, DSA 731-1, June 2, 2005 Conectiva Security Advisory, CLSA-2005:962, June 6,

	Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/Owl/CHANGES-current.shtml SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.23 SGI IRIX: Apply patch 5892 for IRIX 6.5.24-6.5.27: ftp://patches.sgi.com/support/free/security/patches/ Debian: http://security.debian.org/pool/updates/main/k/krb4/		2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 **Avaya Security Advisory, ASA-2005-132, June 14, 2005**

	Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000962 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-132_RHSA-2005-327.pdf** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors MPlayer 1.0pre6 & prior; Xine 0.9.9-1.0; Peachtree Linux release 1	Several vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to a boundary error when processing lines from RealMedia RTSP streams, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported due to a boundary error when processing stream IDs from Microsoft Media Services MMST streams, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff Gentoo: http://security.gentoo.org/glsa/glsa-200504-19.xml Patches available at: http://cvs.sourceforge.net/viewcvs.py/xine/xinelib/src/input/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-27.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Desktop/** Currently we are not aware of any exploits for these vulnerabilities.	MPlayer RTSP & MMST Streams Buffer Overflow CAN-2005-1195	High	Security Tracker Alert,1013771, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-19, April 20, 200 Peachtree Linux Security Notice, PLSN-0003, April 21, 2005 Xine Security Announcement, XSA-2004-8, April 21, 2005 Gentoo Linux Security Advisory, GLSA 200504-27, April 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 Slackware Security Advisory, SSA:2005-121-02, May 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:013, May 18, 2005 **Turbolinux Security Advisory, TLSA-2005-65, June 15, 2005**
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	**US-CERT VU#222750** Sun(sm) Alert Notification, 57746, April 29, 2005 US-CERT VU#415294 Security Focus, 13124, May 21, 2005

	efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1 ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Squid Web Proxy Cache 2.3, STABLE2, STABLE4-STABLE7, 2.5, STABLE1, STABLE3-STABLE9	A remote Denial of Service vulnerability has been reported when a malicious user prematurely aborts a connection during a PUT or POST request. Patches available at: http://www1.uk.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-post.patch Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-415.html** There is no exploit code required.	Squid Proxy Aborted Connection Remote Denial of Service CAN-2005-0718	Low	Security Focus, 13166, April 14, 2005 Turbolinux Security Advisory, TLSA-2005-53, April 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:078, April 29, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 **RedHat Security Advisory, RHSA-2005:415-16, June 14, 2005**
Multiple Vendors Netscape Netscape 8.0.1; Mozilla Firefox 1.0-1.0.4, 0.10.1, 0.10, 0.9-0.9.3, 0.8, Firefox Preview Release; Mozilla Browser 1.8 Alpha 1-Alpha 4, 1.7.8 Mozilla Browser 1.7- 1.7.7, 1.6, 1.5.1, 1.5, 1.4.4, 1.4.2, 1.4.1, 1.4, 1.4 a & b, 1.3.1, 1.3, 1.2.1, 1.2, Alpha & Beta, 1.1, Alpha & Beta, 1.0-1.0.2, 0.9.48, 0.9.35, 0.9.9, 0.9.2-0.9.8, 0.8, M16, M15; Camino 0.x	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Multiple Vendors Mozilla/Firefox Browsers Dialog Box Origin Spoofing	Medium	Secunia Advisory, 21, 2005

ObsidianX amaroK Web Frontend 1.3 (plugin for amaroK)	A security issue has been reported that could let remote malicious users view sensitive information. This is because configuration settings are stored in the file 'globals.inc' inside the web root, which may allow disclosure of the username and password for the underlying database. Update to version 1.3.1: http://sourceforge.net/project/showfiles.php?group_id=141248 Currently we are not aware of any exploits for this vulnerability.	ObsidianX amaroK Web Frontend Credential Exposure CAN-2005-2029	Medium	Secunia SA15736, June 17, 2005
Opera Software Opera 8.0	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks and read local files. This is due to Opera not properly restricting the privileges of 'javascript:' URLs when opened in e.g. new windows or frames. Update to version 8.01: http://www.opera.com/download/ There is no exploit code required.	Opera 'javascript:' URL Cross-Site Scripting CAN-2005-1669	High	Secunia, SA15411, June 16, 2005
Opera Software Opera 8.0	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to improper input validation when Opera generates a temporary page for displaying a redirection when 'Automatic redirection' is disabled (not default setting). Update to version 8.01: http://www.opera.com/download/ Currently we are not aware of any exploits for this vulnerability.	Opera Redirection Cross-Site Scripting	High	Secunia SA15423, June 16, 2005
Opera Software Opera 8.0	A vulnerability has been reported that could let remote malicious users steal content or perform actions on other web sites with the privileges of the user. This is due to insufficient validation of server side redirects. Update to version 8.01: http://www.opera.com/download/ Currently we are not aware of any exploits for this vulnerability.	Opera XMLHttpRequest Security Bypass CAN-2005-1475	Medium	Secunia SA15008, June 16, 2005
Opera Software Opera 7.x, 8.x	A vulnerability has been reported because JavaScript dialog boxes don't display/include their origin, which could let a remote malicious user spoof dialog boxes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Opera Web Browser Dialog Box Origin Spoofing	Medium	Secunia Advisory, SA15488, June 21, 2005
osCommerce osCommerce 2.2 ms1&ms2, 2.2 cvs, 2.1	Multiple HTTP response splitting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could lead to a false sense of trust. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	osCommerce Multiple HTTP Response Splitting CAN-2005-1951	Medium	Security Focus, 13979, June 17, 2005
Outburst Production Ultimate PHP Board 1.9.6 GOLD & prior	Multiple input validation vulnerabilities were reported that could let a remote malicious user conduct cross-site scripting attacks. These are due to errors in the following scripts: 'login.php,' 'viewtopic.php.' 'profile.php.' 'newpost.php.' 'email.php.' 'icq.php.' 'aol.php.' 'getpass.php.' and 'search.php.' Workaround available at: http://www.myupb.com/forum/viewtopic.php?id=26&t_id=118 There is no exploit code required; however, a Proof of Concept exploit has been published.	Outburst Production Ultimate PHP Board Cross-Site Scripting CAN-2005-2003 CAN-2005-2004 CAN-2005-2005	High	Security Focus, 13971, June 16, 2005
Outburst Production Ultimate PHP Board 1.9.6, 1.9, 1.8.2, 1.8	A vulnerability has been reported due to a weak password encryption scheme, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing.	Outburst Production Ultimate PHP Board Weak Password Encryption	Medium	Security Focus, 13975, June 16, 2005

	An exploit script has been published.	CAN-2005-2030		
peercast.org PeerCast 0.1211	A format string vulnerability has been reported when attempting to handling a malformed HTTP GET request, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrade available at: http://www.peercast.org/download.php **Gentoo:** **http://security.gentoo.org/glsa/glsa-200506-15.xml** A Proof of Concept exploit has been published.	Peercast.org PeerCast Remote Format String CAN-2005-1806	High	GulfTech Security Research , May 28, 2005 **Gentoo Linux Security Advisory, GLSA 200506-15, June 20, 2005**
PHP Arena paFaq Beta4	Multiple vulnerabilities have been reported: multiple Cross-Site Scripting vulnerabilities have were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; several SQL Injection vulnerabilities were reported when magic quotes gpc is off which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported which could let a remote malicious user download the entire paFaq database and obtain administrative access; and a vulnerability was reported due to insufficient checking for a valid language pack, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published and an exploit script has been published for the database access vulnerability.	paFaq Multiple Vulnerabilities CAN-2005-2011 CAN-2005-2012 CAN-2005-2013 CAN-2005-2014	High	GulfTech Security Advisory, June 20, 2005
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000957 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-136_RHSA-2005-405_RHSA-2005-406.pdf** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass CAN-2004-1392	Medium	Security Tracker Alert ID, 1011984, October 28, 2004 Ubuntu Security Notice, USN-66-1, January 20, 2005 Ubuntu Security Notice, USN-66-2, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 Conectiva Security Advisory, CLSA-2005:957, May 31, 2005 **Avaya Security Advisory, ASA-2005-136, June 14, 2005**
PHP Group PHP prior to 5.0.4; Peachtree Linux release 1	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian:	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory,

	http://security.debian.org/pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ Debian: http://security.debian.org/pool/updates/main/p/php4/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955 Apple: http://www.apple.com/support/downloads/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-136_RHSA-2005-405_RHSA-2005-406.pdf** Currently we are not aware of any exploits for these vulnerabilities.			DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Debian Security Advisory, DSA 729-1, May 26, 2005 Conectiva Security Advisory, CLSA-2005:955, May 31, 2005 Apple Security Update, APPLE-SA-2005-06-08, June 8, 2005 **Avaya Security Advisory, ASA-2005-136, June 14, 2005**
Qualiteam Corp. X-Cart 4.0.8	Some input validation vulnerabilities have been reported due to insufficient validation of user-supplied input in several parameters, which could let a remote malicious user execute arbitrary SQL commands or arbitrary HTML and script code. **The latest version of the application is not vulnerable to these issues as well. Please contact the vendor to obtain fixes.** There is no exploit code required; however, Proofs of Concept exploits have been published.	Qualiteam X-Cart SQL Injection & Cross-Site Scripting CAN-2005-1822 CAN-2005-1823	High	SVadvisory#7, May 29, 2005 **Security Focus, 13817, June 17, 2005**
RealVNC RealVNC 4.0	A vulnerability has been reported when a null session is established, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	RealVNC Server Remote Information Disclosure	Medium	Security Tracker Alert, 1014237, June 19, 2005
socialMPN socialMPN	Multiple input validation vulnerabilities have been reported that could let a remote malicious user inject SQL commands and determine the installation path.	socialMPN SQL Injection	High	Security Tracker Alert ID: 1014214, June 16, 2005

	No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	CAN-2005-2031		
SquirrelMail SquirrelMail 1.4.0 through 1.4.4	Multiple vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting attacks. Upgrade to 1.4.4 and apply patch: http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch Gentoo: http://security.gentoo.org/glsa/glsa-200506-19.xml There is no exploit code required.	SquirrelMail Cross-Site Scripting Vulnerabilities CAN-2005-1769	High	SquirrelMail Advisory, June 15, 2005 Gentoo Linux Security Advisory, GLSA 200506-19, June 21, 2005
Sun Microsystems Sun Solaris 9, 8, 7	A vulnerability has been reported that could let local malicious users overwrite arbitrary files on a vulnerable system. The vulnerability is caused due to an unspecified error in the lpadmin utility. Patches available: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101768-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris lpadmin Arbitrary File Overwrite CAN-2005-2032	High	Sun Advisory 101768, June 15, 2005
Sun Microsystems, Inc. Java Web Start 1.x, Sun Java JDK 1.5.x, 1.4.x, Sun Java JRE 1.4.x, 1.5.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error which could let malicious untrusted applications execute arbitrary code; and a vulnerability was reported due to an unspecified error which could let a malicious untrusted applets execute arbitrary code. Upgrades available at: http://java.sun.com/j2se/1.5.0/index.jsp http://java.sun.com/j2se/1.4.2/download.html **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-current/** Currently we are not aware of any exploits for these vulnerabilities.	Java Web Start / Sun JRE Sandbox Security Bypass CAN-2005-1973 CAN-2005-1974	High	Sun(sm) Alert Notification, 101748 & 101749, June 13, 2005 **Slackware Security Advisory, SSA:2005-170-01, June 20, 2005**

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Another Use For Wi-Fi: Finding Stolen Laptops**: Skyhook Wireless has developed technology that uses Wi-Fi to find stolen mobile devices. This is a positive step in the war against identity thieves and other cybercriminals. The vendor claims that its product is the first positioning system to use Wi-Fi rather than satellite or cellular-based technologies. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=164901191.
- **Hot-Spots Now Number More Than 65,000 Worldwide:** There are now more than 65,000 hotspots in 100 countries, according to a listing released Tuesday by wireless information and service provider JiWire. The United States has the largest number of hotspots with almost 27,600, according to JiWire. The U.K. is in second place with almost 10,500 hotspots and Germany is in third place with almost 6200 hotspots. Source: http://www.informationweek.com/showArticle.jhtml?articleID=164901437

Wireless Vulnerabilities

- **Bluetooth_dot_dot.txt:** An update on dot dot attacks against Bluetooth devices.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
June 21, 2005	claroline16.txt KCcol-xpl.pl	Yes	Exploit for the Claroline remote password hash extraction SQL injection vulnerability.
June 21, 2005	flatnuke_253_referer.pm.gz	Yes	Exploit for the FlatNuke Referer poisoning remote command execution vulnerability.
June 21, 2005	invisionXSSSQL.txt invisionGallery.txt	Yes	Detailed exploitation for the Invision Community Blog Cross-Site Scripting & SQL Injection vulnerability.
June 21, 2005	p33r-b33r.c	Yes	Script that exploits the Peercast.org PeerCast Remote Format String vulnerability.
June 21, 2005	r57mercury.pl	No	Perl script that exploits the MercuryBoard 'Index.PHP' Remote SQL Injection vulnerability.
June 20, 2005	paFaq-add-admin-poc.pl pafaq.pl.txt	No	Exploits for the PAFaq Database Unauthorized Access vulnerability.
June 20, 2005	pictosniff-0.2.tar.bz2	N/A	PictoSniff allows you to spy live on PictoChat communications between Nintendo DS gaming consoles.
June 18, 2005	amap-5.1.tar.gz	N/A	A next-generation scanning tool that allows you to identify the applications that are running on a specific port.
June 18, 2005	CAU-launchd.c	No	Mac OS X 10.4 launchd race condition exploit.
June 18, 2005	CAU-netpmon.c	Yes	Exploit for the IBM AIX 'Netpmon' Command Buffer Overflow vulnerability.
June 18, 2005	CAU-paginit.c	Yes	Script that exploits the IBM AIX paginit Buffer Overflow vulnerability.
June 18, 2005	epsxe-e.c	No	Exploit code that uses a locally exploitable stack overflow in ePSXe to gain root privileges.
June 18, 2005	hydra-4.7-src.tar.gz	N/A	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more that includes SSL support, parallel scans, and is part of Nessus.
June 18, 2005	invision.php.txt	Yes	Exploit for the Invision Power SQL Injection vulnerability.
June 18, 2005	ipswitch.c	Yes	Exploit for the IpSwitch IMAP server LOGON stack overflow vulnerability.
June 18, 2005	KAV_exploit.cpp	No	Exploit for the Kaspersky Anti-Virus Klif.Sys Privilege Escalation Vulnerability.
June 18, 2005	KCpnuke-xpl.pl	Yes	Perl script that exploits the PostNuke versions 0.750 SQL Injection vulnerability.
June 18, 2005	M4DR007.pl Webhints.c Webhints.pl	No	Perl script that exploits the Darryl Burgdorf Webhints Remote Command Execution vulnerability.
June 18, 2005	mambo4521.php.txt	Yes	Exploit for the Mambo 4.5.2.1 + MySQL 4.1 fetch password hash vulnerability.
June 18, 2005	memfs.c	Yes	Proof of Concept exploit for the FUSE Information Disclosure vulnerability.
June 18, 2005	mimedefang-2.52.tar.gz	N/A	A flexible MIME email scanner designed to protect Windows clients from viruses.
June 18, 2005	MIRC.PAS.HTML	No	Exploit for the MIRC 6.16 and 'generic Edit component' Win32 vulnerability.
June 18, 2005	paFileDB113.pl.txt	Yes	Exploit for the PHP Arena paFileDB Password vulnerability.
June 18, 2005	portalSQL.pl.txt	No	Exploit for the PortailPHP ID Parameter SQL Injection vulnerability.
June 18, 2005	radexecd.txt	No	Detailed exploitation for the HP OpenView Radia Buffer Overflows vulnerabilities.
June 18, 2005	rakzero.zip	Yes	Proof of Concept exploit for the Rakkarsoft RakNet Remote Denial of Service vulnerability.
June 18, 2005	spa-promail4.c	Yes	Exploit for the SPA-PRO Mail @Solomon IMAP Server Buffer Overflow Vulnerability.
June 18, 2005	tcpdump-bgp-update-poc.c	Yes	Denial of Service exploit for the TCPDump BGP Decoding Routines vulnerability.
June 18, 2005	tftp_exp.c	No	Denial of Service exploit for the FutureSoft TFTP Server 2000 Directory vulnerability.
June 18, 2005	THCsnooze-0.0.7.tar.gz	N/A	A next-generation sniffing tool that supports modularized protocol dissectors and remote log file retrieval.
June 18, 2005	UPBdecrypt.pl.txt password_decrypter_UPB.pl	No	Exploit for the Ultimate PHP Board Weak Password Encryption vulnerability.
June 18, 2005	webstore.pl.txt	No	Exploit for the eXtropia WebStore Remote Command Execution vulnerability.
June 18, 2005	winzipBO.c	No	Exploit for the WinZip Local Buffer Overflow vulnerability.
June 18, 2005	wordpressSQL.txt	Yes	Exploit for the Wordpress Cat_ID Parameter SQL Injection vulnerability.
June 17, 2005	virobot_ex.pl	No	Exploit for the ViRobot Linux Server Remote Buffer Overflow vulnerability.

[back to top]

Trends

- **Browser Windows Without Indications of Their Origins may be Used in Phishing Attempts:** Microsoft has investigated a public report of a phishing method that affects Web browsers in general, including Internet Explorer. The report describes the scenario of multiple, overlapping browser windows, some of which contain no indications of their origin. An attacker could arrange windows in such a way as to trick users into thinking that an unidentified dialog or pop-up window is trustworthy when it is in fact fraudulent. Source: Microsoft Security Advisory (902333) Browser Windows Without Indications of Their Origins may be Used in Phishing Attempts.
- **Spyware Danger Meets Rootkit Stealth:** According to spyware experts, that the makers of one common spyware program are borrowing techniques from another type of malicious program, known as "rootkits," to help evade detection on systems they infect. Recent versions of the Cool Web Search spyware have rootkit-like features that allow the spyware authors to hide their program files on Windows systems. Source: http://www.eweek.com/article2/0,1759,1829744,00.asp?kc=EWRSS03129TX1K0000614.
- **Pharming, phishing remain major online fraud threats, VeriSign says:** According to VeriSign Inc.'s most recent Internet security intelligence briefing, pharming is emerging as a major method of online fraud. The briefing is based on transactions settled by VeriSign during the first quarter. Pharming tricks a user's computer into connecting to a fake web site even if the correct domain name information is entered into the browser. The technique exploits vulnerabilities in domain name service software to distribute fake address information, VeriSign says. Source: http://internetretailer.com/dailyNews.asp?id=15253.
- **Banks Not Doing Enough To Stop ID Theft:** According to a report by Javelin Strategy & Research, most financial institutions that provide credit cards are doing an inadequate job of attacking the problem, focusing on resolution rather than prevention and detection. The report ranked leading card-issuing banks based on three criteria: prevention, detection, and resolution. Issuers could score a maximum of 100 points: 40 points each for prevention and detection, and 20 points for resolution. The rankings were based on a survey of 39 banks in which researchers posing as customers asked about the bank's ID theft policies. Prevention and detection were weighted more heavily than resolution because of their greater potential benefits and cost savings. Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=BFCBD0OR2YWQQQSNDBGCKH0CJUMEKJVN?articleID=164303598#.
- **Browser-based attacks increase as viruses dip:** The Computing Technology Industry Association, or CompTIA, released its third annual report on IT security and the work force. The survey of nearly 500 organizations, found that 56.6 percent had been the victim of a browser-based attack, up from 36.8 percent a year ago and a quarter two years ago. Browser-based attacks often take advantage of security flaws in Web browsers and other components of the user's PC such as the operating system. The attackers' objective can be to sabotage a computer or steal private data, and the attacks can be launched when a person visits a Web page that appears harmless but contains malicious code. Source: http://news.com.com/Browser-based+attacks+increase+as+viruses+decrease/2100-7349_3-5747050.html#talkback.
- **Identity thieves go big business:** Authorities state that they've noted an increase in more sophisticated scams in which identity thieves steal the names and larger credit lines of businesses and nonprofit groups. Called "corporate identity theft,' the crime is growing rapidly, according to Whittier-area state Assemblyman Ron Calderon, D-Montebello, who has introduced a bill to help fight the problem. Corporate identity thieves can rip off companies and nonprofit organizations for thousands of dollars at a time. The thieves will typically gain access to a firm's credit card information and use it to pile up hefty bills, officials sa. Source: http://www.pasadenastarnews.com/Stories/0,1413,206~22097~2921031,00.html
- **Trojan Horse E-Mails Suggest Trend Toward Targeted Attacks:** The UK's National Infrastructure Security Co-Ordination Center released a report disclosing that more than 300 government departments and businesses were targeted by a continuing series of e-mail attacks designed to covertly gather sensitive and economically valuable information. The report highlights an emerging trend away from mass-mailing worms and viruses to far more targeted ones. Source: http://www.snpx.com/cgi-bin/news55.cgi?target=99127134?-2622.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
2	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
3	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
4	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

5	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
6	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
7	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
8	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
9	Netsky-B	Win32 Worm	Stable	February 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. Also searches drives for certain folder names and then copies itself to those folders.
10	MyDoom-O	Win32 Worm	Stable	July 2004	A mass-mailing worm that uses its own SMTP engine to generate email messages. It gathers its target email addresses from files with certain extension names. It also avoids sending email messages to email addresses that contain certain strings.

Table Updated June 21, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Nothing significant to report.

[back to top

Last updated June 22, 2005